Assuring the USAF Core Missions in the Information Age

Lt Gen William J. Bender, USAF
Col William D. Bryant, USAF

The United States Air Force was unquestionably the world's premier and most powerful air force in the industrial age. Our challenge and opportunity are to translate that effectiveness and capability to defend our nation into the information age. To accomplish this, we must be able to execute our five core missions of air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control in and through cyberspace. While our environment has changed continuously and rapidly throughout history, these enduring missions have remained our focus. We have always had to protect and

defend our capability to accomplish these missions; what has changed is our necessity to protect and assure them via the information-age domain of cyberspace.

Freedom of action in cyberspace through the application of mission assurance is a prerequisite for successful Air Force core mission execution. Obtaining and maintaining freedom of action will prevent the enemy from effectively interfering with operations. Doing so also allows the Air Force to deliver precise combat power by exploiting cyberspace's unique characteristics. Cyberspace is often poorly understood, and its unique characteristics may cause much confusion over how to best assure our core missions through cyberspace.

The Joint Staff has defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] This definition clarifies that cyberspace is much more than just traditional computer networks. While the Internet is part of cyberspace, it is not all of cyberspace. Any computer system capable of communicating with other computer systems in some way is part of cyberspace. A desktop computer, an avionics computer on an aircraft, a smart phone, an industrial controller, and the processors on a modern car are all part of cyberspace, although only some of them are routinely connected to the Internet. Most modern military equipment—from a humble truck to a B-2 bomber—has some form of processor and is thus reliant upon and a part of cyberspace.

Cyberspace is unique in that it is man-made and can be changed and modified easier than the physical domains of land, sea, air, and space. Gregory Rattray has noted that while mountains and oceans cannot be moved by combatants, in cyberspace a combatant can move or even turn off the equivalent geographic features with the flip of a switch.[2] This extreme mutability has caused some analysts to consider cyberspace to be a purely virtual domain, but this is a critical mistake.

Cyberspace is composed of information and connections in a virtual space but is grounded in the physical world.[3] According to cyberspace analyst Paul Rosenzweig, "We should never forget that though the cyber domain is an artificial one created by man, it exists only in the context of the fundamental natural domain of the world."[4] Events in the physical world affect cyberspace. If the heart of cyberspace is the connections between computing devices, then anything that impacts those devices or their connections alters cyberspace. A failed air conditioning unit at a server farm, a backhoe cutting a fiber cable, or an anchor dragging across an undersea cable can have a tremendous effect on the digital terrain. Even more important for assuring the Air Force core missions is the shared comprehension of cyberspace dependencies upon physical components.

Every one of the critical systems by which we accomplish our core missions is built upon cyberspace capabilities. Aircraft, satellites, trucks, and ICBMs all rely upon our ability to maneuver and operate within cyberspace. Some analysts have suggested that there is no such thing as maneuver in cyberspace since computers simply execute their instructions, even if those instructions include the ability to respond to stimuli. While computers do not maneuver, people do, and conflict in the cyberspace domain is fought by a melding of inflexible silicon and flexible people

telling the silicon what to do. Accordingly, conflict in the cyberspace domain remains driven by humans who make decisions and react to their adversaries in ways that would still be familiar to Clausewitz and other traditional military thinkers.[5] If we are to be successful in the cyberspace domain, we cannot rely solely upon "if-then" logic and engineering solutions. We must maneuver in and through cyberspace, but to do so effectively, we must start by developing our people.

Creating a proficient cadre of cyberspace operators is one of my top priorities. We are working hard to identify necessary skill sets and determine how to best develop the career field. However, change must go beyond cyberspace operators. Everyone in the total force must learn to think of cyberspace as a war-fighting domain, and mission assurance is not something created by technical experts alone. Every Airman who plugs an unauthorized device into a network or circumvents a security control on a maintenance loader needs to understand that he or she is creating vulnerabilities for our enemies to exploit. Our adversaries could implant weapons, resulting in our inability to accomplish our missions and, ultimately, the death of brave Americans in combat. Everything is connected, and that questionable e-mail link can unleash a weapon that crosses into mission systems. The fact that some of our systems do not use commercial operating systems such as Windows is no defense against a competent and well-resourced adversary. We must also shift our thinking away from trying to prevent every attack and towards how we are going to fight through attacks while still accomplishing our missions.

Cyberspace resilience will be the key to flying, fighting, and winning in a contested cyberspace environment. Therefore, cyberspace operators need to move beyond asking, "How can I best secure this system against attack?" to "How do I operate in a cyber-contested environment where the enemy will get through at least some of my defenses?" This requires a significant mind-set shift for military cyberspace operators, to include focusing on response capabilities such as emergency and incident-response teams and plans.[6] One of the best ways to accomplish this shift is through aggressive and thorough red teaming. A red team is a group of friendly attackers who attempt to attack systems to find their vulnerabilities and weaknesses. They use the same techniques as real-world attackers and provide an invaluable service in not only finding vulnerabilities but also giving defenders practice in how to recognize and respond to attacks to keep their systems functioning. Red teams are crucial in large-scale exercises that are unscripted and prepare defenders to deal with high-level maneuvering adversaries. Shifting to a resiliency-focused defense involves a paradigm shift that is difficult for most military personnel. Antoine Bousquet has highlighted the US military's tendency to strive for " '100% relevant content, 100% accuracy, and zero time delay' which would allow the perfect operation of a frictionless cybernetic war machine."[7] Resilience instead calls for embracing uncertainty and designing for the ability to adapt to failure and the unforeseen. The supposed revolution in military affairs that was going to dissipate the Clausewitzian "fog" through perfect information has largely been discredited, but it still echoes in US military cultural preferences to pursue perfect information. It is not just the cyberspace warriors who need to adapt; operators and support personnel who focus on the physical domains also need to practice operating effectively in an environment of constant change where not everything works as expected. Although this

training is easiest for defenders to accomplish in difficult exercise scenarios, we sometimes shy away from such scenarios due to a cultural fear of failure. When is the last time a US military unit fought an exercise "war" with none of its computers working? All too often the red team's hands are tied to preclude the fulfillment of exercise objectives. However, there has yet to be a war in which the enemy followed the script and did what was expected. Thus, we must practice as we believe we will fight in a volatile, uncertain, complex, and ambiguous (VUCA) environment. Hence, a realistic battlefield that accurately represents the future environments is essential for combatants to prepare for failure and be able to continue fighting, even if they temporarily lose some of their war-fighting systems.

Under the direction of the USAF chief of staff, I convened Task Force Cyber Secure to assure the five core missions and maintain our effectiveness in the information age. The task force teamed cyberspace operators with our operations and intelligence teammates to integrate efforts across the Air Force and focus on concrete steps to leverage opportunities while managing our risks within cyberspace. The task force helped to diagnose the problem, started an absolutely essential cross-functional dialogue, and looked hard at how to advance education and culture in cyberspace across the Air Force. In addition, the task force is setting up an enduring framework to continue moving forward that includes an Air Force chief information security officer (CISO), changes to governance and funding, and an enduring focus on mission assurance in cyberspace. We cannot afford to wait as our adversaries continue to improve their ability to hold our core missions at risk, and it will require all of us across the total force to ensure that we continue to be the world's premier air force into the information age. ✪

Notes

1. Joint Publication 3-13, *Information Operations*, 27 November 2012 (incorporating change 1, 20 November 2014), II-9, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

2. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 256.

3. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 18–19.

4. Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), 20.

5. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

6. Rattray, *Strategic Warfare in Cyberspace*, 209.

7. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 222.

Lt Gen William J. Bender, USAF

Lieutenant General Bender (BE, Manhattan College; MA, Embry-Riddle Aeronautical University; MA, US Army War College) is chief of the Office of Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, DC. General Bender leads three directorates and supports 54,000 cyber operations and support personnel across the globe with a portfolio valued at $17 billion. He has overall responsibility for the Air Force's information technology portfolio as the senior authority for information technology investment strategy, networks, and network-centric policies, communications, information resources management, information assurance, and related matters for the Department of the Air Force. As chief information officer, General Bender provides oversight of portfolio management, delivers enterprise architecture, and enforces Freedom of Information Act and Privacy Act laws. He integrates Air Force war-fighting and mission-support capabilities by networking air, space, and terrestrial assets. Additionally, he shapes doctrine, strategy, and policy for all cyberspace operations and support activities.

Col William D. Bryant, USAF

Colonel Bryant (USAFA; MA, American Military University; MA, George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], PhD, School of Advanced Air and Space Studies; MSS [Master of Strategic Studies], Air War College) is the deputy director, Task Force Cyber Secure for the Office of Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, DC. A career fighter pilot and strategist, he has served in numerous operational and staff assignments.

Let us know what you think! Leave a comment!

http://www.airpower.au.af.mil